DEPARTMENT OF THE NAVY
COMMANDER
SECOND NAVAL CONSTRUCTION BRIGADE
NAVAL AMPHIBIOUS BASE, LITTLE CREEK
NORFOLK, VIRGINIA 23521-5070
AND
COMMANDER
THIRD NAVAL CONSTRUCTION BRIGADE
PEARL HARBOR, HAWAII 96860-7305

COMSECONDNCB/COMTHIRDNCBINST 2000.1
N6
18 NOV 1998

COMSECONDNCB/COMTHIRDNCB INSTRUCTION 2000.1

Subj: INTERNET POLICY

Ref: (a) DOD Directive 5500.7-R, Section 2-301 (Joint Ethics Regulations)
(b) ALPACFLT/ALLANTFLT 210151Z Feb 98
(c) SECNAV (SECNAV 211930Z Oct 98) Department of the Navy Worldwide Web Policy
(d) OPNAVINST 5239.1A ADP Security Policy
(e) The Privacy Act of 1974, 5 U.S.C. Section 552A

Encl: (1) Sample NAVPERS 1070/613, Administrative Remarks

1. Purpose. To establish COMSECONDNCB/COMTHIRDNCB policy on Internet access and use of Government Information Systems.

2. Background. Information systems and Internet applications can improve many facets of our operations and provide an efficient and effective means of communication and information distribution.

3. Policy

a. COMSECONDNCB/COMTHIRDNCB will promote the widest permissible use of Government Information Systems to access and exchange information in an automated environment. Personnel assigned to NCF units, military and civilian, are encouraged to use their government computers to access the Internet and develop information skills.

b. The best way to develop information technology skills is to get on the Internet and make it the preferred choice to access, develop and exchange information, as supported by reference (a). Fleet policy, as presented in reference (b), is that any permissible use of the Internet enhances the users'

professional skills and thus serves a legitimate public interest.

c. Use of Government Information Systems is both an essential work requirement and a personal privilege. All COMSECONDNCB/COMTHIRDNCB personnel are reminded that Commanding Officers and Officers in Charge (CO/OIC) have the authority to control or limit the use of Government Information Systems to include blocking specific sites, limiting or restricting Internet or Email access due to resource constraints, or revoking an individual's use altogether.

d. Permissible use of Government Information Systems is defined as that not prohibited by law, regulation, instruction or command policy. Prohibited uses as derived from reference (a) and amplified in reference (b), include:

(1) Introducing classified information into an unclassified system or environment.

(2) Accessing, storing, processing, displaying, distributing, transmitting or viewing material that is pornographic, racist, promotive of hate crimes, or subversive in nature.

(3) Storing, accessing, processing or distributing classified, propriety, sensitive, For Official Use Only (FOUO) or Privacy Act protected information in violation of established security and information release policies.

(4) Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.

(5) Knowingly writing, coding, compiling, storing, transmitting or transferring malicious software code, to include viruses, logic bombs, worms and macro viruses.

(6) Promoting partisan political activity.

(7) Disseminating religious materials outside an established command religious program.

(8) Using the system for personal financial gain, such as advertising or solicitation of services or sale of personal property, with the exception of utilizing a command approved

mechanism such as a welfare and recreation electronic bulletin board for advertising personal items for sale.

(9) Promoting or advertising fund raising activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g. welfare and recreation car washes).

(10) Writing, forwarding or participating in chain letters.

(11) Posting personal home pages.

(12) Personal encryption of electronic communications.

e. Units are encouraged to generate home pages to post unit specific information. Reference (c) outlines the requirements and limitations of Navy home pages. The following specific COMSECONDNCB/COMTHIRDNCB requirements and limitations apply to unit home pages:

(1) Home Page Server. Unit home pages must reside on a military server that is maintained in strict compliance with reference (d) ADP Security Policy.

(2) Brigade Oversight. Unit home pages will be coordinated by Brigade Information Technology Staffs (N6). The Brigade N6's must approve any web site related costs in writing. Units may not directly fund, or accept free, commercial home page services. Units will not provide photographs, articles, logos, history, instructions, or any informational material to any individual or company for the purpose of creating, maintaining, or fostering an unofficial or unauthorized web site. Any unit-originated material published on the Internet must strictly comply with DON worldwide web policy (see reference (c)).

(3) Unit Webmaster. Every unit web site must have a Webmaster and an alternate Webmaster designated in writing by the CO or OIC. The Webmaster is usually either the unit ADP Officer (S6), or the PAO. Online feedback from the web site must be checked daily by the unit Webmaster, or the alternate in the absence of the primary. This is most efficiently done via a direct Email link to the Webmaster.

(4) Posting Information. The unit PAO will screen, edit as necessary, and recommend to the CO/OIC approval/disapproval

for any information (including photos, articles, schedules, cartoons, data etc.) destined to be posted to the home page. The unit CO/OIC must approve all release of information to the home page. The unit Webmaster is the only one authorized to post information to the unit home page, and must develop internal procedures and LAN safeguards to ensure PAO, ADPSO, and CO/OIC approval prior to release of information. COs and OICs are reminded that any information posted to the Internet is a direct reflection on their Command, the Seabees and the Navy. The utmost care must be exercised to ensure all internet "broadcasted" information is appropriate for release and does not compromise unit or force security or personal privacy act protected information (see reference (e) for Privacy Act guidelines).

(5) Periodic Update. Unit COs and OICs are responsible for the quality, timeliness, and relevancy of information posted on their Web site. At least once each month, the Webmaster and PAO will review the entire home page and recommend changes to the CO/OIC. In general, information greater that six (6) months old should be moved to an archive site (6-24 month old info) or incorporated into the unit history section of the home page. The date of the last home page revision will be included with the Webmaster code, name, phone number and Email address.

f. All government computer systems are subject to monitoring, recording, and periodic audits to ensure they are functioning properly and to protect against unauthorized use. Failure to comply with the policy set forth in this instruction or any attempt to disable, defeat, or circumvent security measures may result in disciplinary action.

g. A number of free Email services are available and can be found by conducting an Internet search for free Email. Use of these free services is encouraged for electronically communicating with family and friends when deployed.

h. Although wide use of Internet services are encouraged as described above, there are applications that are detrimental to the operation and efficiency of the unit network. In general, continuous Internet monitoring of hometown radio stations, live sporting events, online news broadcasts, or live video are discourage and should be minimized. These type of applications require a significant bandwidth to operate, slowing the performance of the server, and hindering official business.

4. Action. COs and OICs shall ensure all personnel are familiar with the policies laid out in this instruction. COs and OICs will ensure all personnel review this instruction and receive initial and periodic security awareness and Internet usage training. Such training will be augmented with new and changing issues regarding security and the Internet. An awareness statement and record of training will be signed by all personnel and will be maintained at the command. This training will be documented using appropriate Page 13 entries such as enclosure (1).

S. E. BARKER
Vice Commander

J. A. MEHULA
Deputy Commander

Distribution:
COMSECONDNCB/COMTHIRDNCBINST 5216.1B
Lists I & II

ADMINISTRATIVE REMARKS
NAVPERS 1070/613(Rev.10-81)
S/N 0106-LF-010-6991

Command Name, Address, UIC

DDMMMYY: I have read the command's Internet instruction and received Internet security and usage training. I fully understand the terms of this policy and agree to abide by them. I realize that command resources are subject to monitoring and that the Internet address of any site that I visit is recorded. I am aware that any use which is illegal, harassing, offensive and/or in violation of other command policies may be the basis for criminal, disciplinary, and administrative action.

Member signature: _____

Instructor signature: _____

NAME (Last, First, MI)	SSN	BRANCH & CLASS

Enclosure (1)